MITNOC
Command Brief

“LEAD WOLF IN THE IT WOLF PACK”

June 2000

Albany fix: “Away Team form the NOC w/ 2 senior firewall engineers, 1 senior router engineer, 1 MCSE

DoD: President’s White Paper, DEPSECDEF Hamery initiative, JCS Cyber Action Plan

USMC: CIO technical direction, IA Vision statement, NOC CONOPS, PP&O position

- MCEN/MITNOC Overview
- **Personnel**
- **MCEN Current Architecture**
- **MCEN Future Architecture**
- **Deployed Support**
- **Defense-In-Depth**
- **MARFOR-CND**

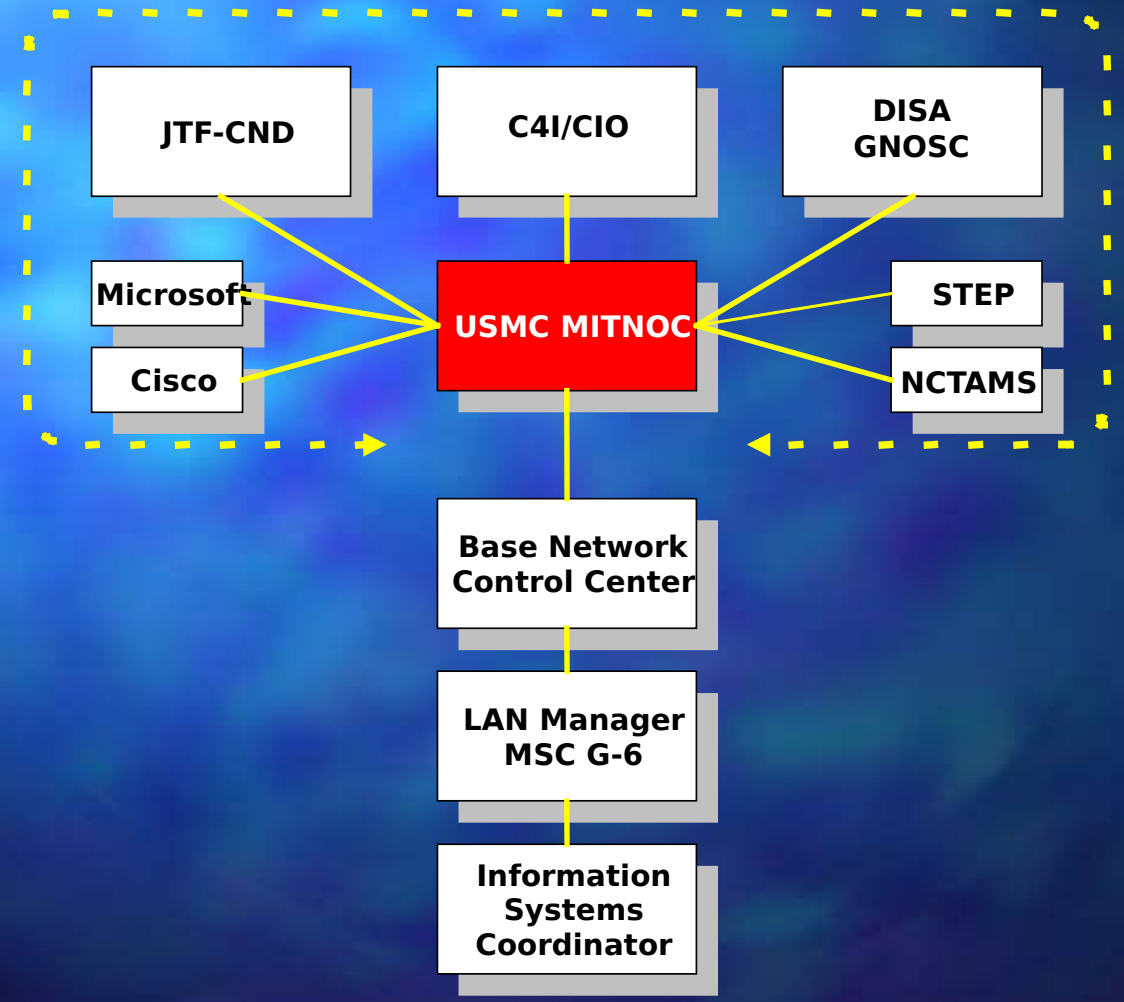
MCEN
What Is IT?

- The Marine Corps Enterprise Network (MCEN) is the Marine Corps global enterprise network which supports all data communication requirements for Marine Forces world-wide to effect information exchange across the Global Information Grid (GIG). It is composed of DISN only connections consisting of 27 NIPRNET (unclassified) and 19 SIPRNET (classified) points of entry spanning from Europe to Korea centrally managed by the MITNOC located in Quantico, VA.

MCEN CONOPS
MITNOC MISSION

- The Marine Corps Enterprise Network (MCEN) provides a global, secure “plug and play” environment that supports critical C2W functions.
- The Marine Information Technology & Network Operations Center (MITNOC) provides continuous, secure, global communications and management of the Marine Corps Enterprise Network (MCEN) for Marine Forces world-wide to affect information exchange across the Global Information Grid (GIG).

MCEN Support Hierarchy



Defining the Focus

MITNOC Vision Statement

- In partnership with our customers, we provide technical leadership and deliver flawless, global information exchange and service excellence…from anywhere, to anyplace, at anytime.

MITNOC PERSONNEL

“For the strength of the Pack is the Wolf, and the strength of the Wolf is the Pack.”

ALMAR 023/99 32nd Commandant’s Planning Guidance

work Centric Warfare and Information Superiority is al
people (intellectual capital) not technology

MITNOC Sections

- Operations Branch
  - VPN
  - MIDAS
    - IDS
    - VAP
    - CIRT
    - Virus
  - WAN/Security Management
    - Firewall
    - Router
    - Application SDLC Consultation
  - Marine Corps Marathon
  - Engineering
    - ATM
    - IP Management
    - Circuits
  - Call Center
  - PKI
  - NOS/Messaging
    - X.400
    - DMS COC
    - 2000 Migration
  - Deployed Support
    - MEF/MEU/DSID
  - MARFOR CND

Technical Support Hierarchy

Customer

Call Center
Trouble Ticket Generation/Assignment

Tier 1 NOS/MSG	Tier 1 WAN/Security	MIDAS
Tier 2 NOS/MSG	Tier 2 WAN/ Security/VPN	Tier 2 Architectural Engineering

MITNOC Section Cont.

- Logistics Branch
  - Contracting
  - Enterprise Maintenance
- Plans & Projects
  - BPR
- Application Support Branch
- Executive Branch

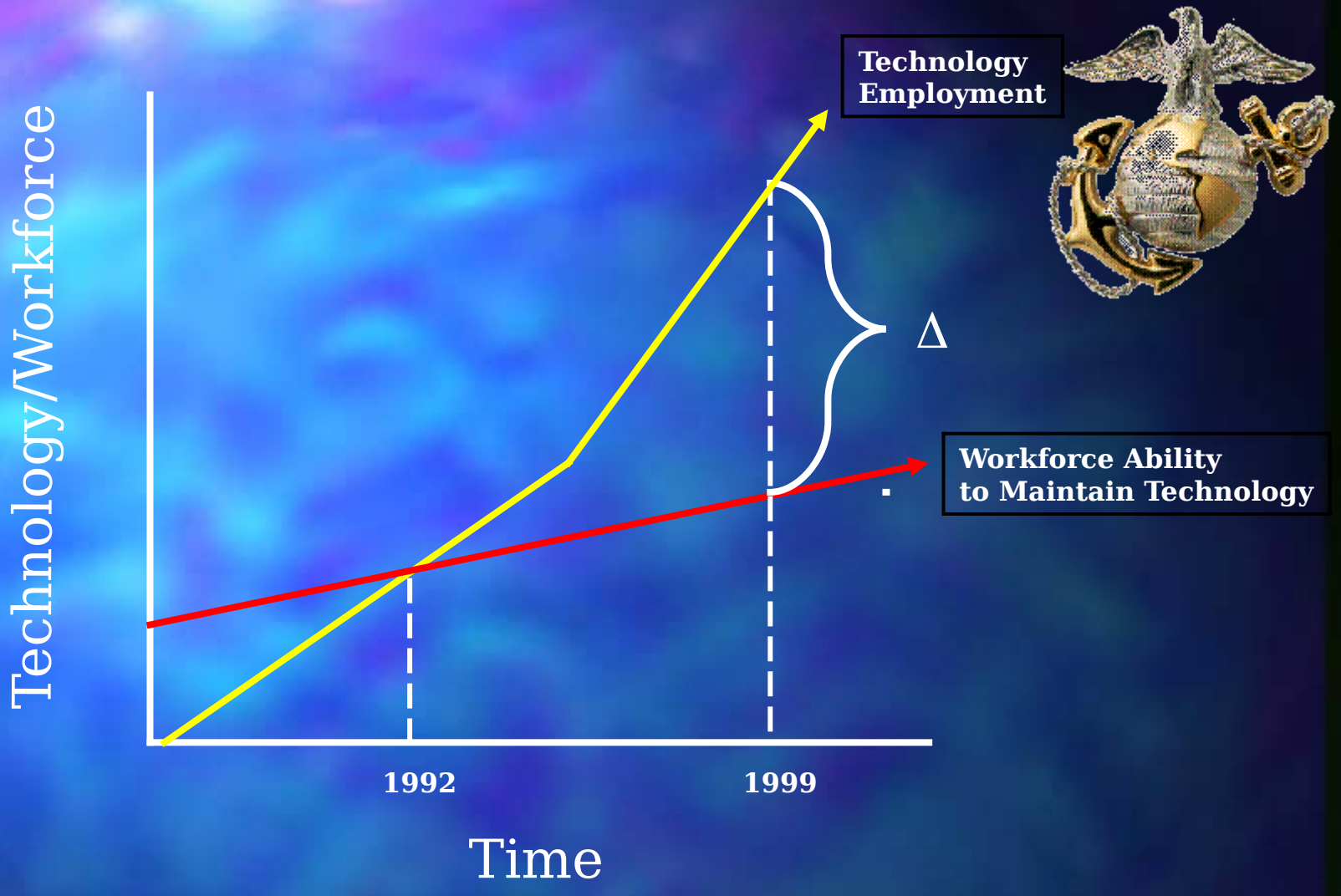
MITNOC Table of Organization

	Officers	Civilians	SNCO/Enlisted
T/O		19	46
32/59			
On-Board	13		38
35/39			

UNITED STATES MARINE CORPS INFORMATION TECHNOLOGY & NETWORK OPERATIONS CENTER

“We must also take full advantage of outsourcing and privatization of functions that contractors can sometimes perform less expensively than federal employees and active duty personnel.”

ALMAR 023/99 32nd Commandant’s Planning Guidance



Represents Marine Corps "green suit" ability to install, operate, and maintain employed tech

Represents the technology employed throughout the Marine Corps that must be installed, op

Δ Contracted Support

MITNOC Contractor Augmentation

- **FY97**
- **On-Site**
  - 6
- **Touch Labor by Location**
  - 1 MCB Camp Pendleton
  - 1 MCB Camp Lejeune
  - 1 MCB Camp Butler
  - 1 MARFORPAC

- **FY00**
- **On-Site**
  - 55
- **Touch Labor by Location**
  - 3 MCB Camp Pendleton
  - 2 MCB Camp Lejeune
  - 3 MCB Camp Butler
  - 2 MARFORPAC
  - 1 MARFORLANT
  - 1 MARFOREUR
  - 1 MCLB Albany

MCEN CURRENT ARCHITECTURE

“I have but one lamp by which my feet are guided, and that is the lamp of experience”

Patrick Henry

“An Enterprise Approach” Multiple Architectures

- **Management Architecture**
  - Provides the pulse of the network
- **Network Architecture**
  - Provides the communication paths
- **Information Assurance Architecture**
  - Ensures the integrity, confidentiality, and availability of the data
- **Information Architecture**
  - The actual flow of information exchange

Management Architecture

Current

- Manned 24X7 Help Desk
- MITNOC HP Openview
- Remedy Help Desk Trouble Ticket System
- MRTG (In House Scripts)
- MCEN Regional Views
- SMS

Future

- Enterprise HP Openview
- Concord Network Health
- TCCC/GNOSC Reporting
- Enterprise Remedy

Network Architecture

Current

- Centralized IP Mgmt
- DISN Only
- Legacy Network Support (Stovepipe Networks)
- Centralized Circuit Mgmt

Future

- SIPRNET Expansion/Extension
- Dynamic Bandwidth Mgmt
- Voice/Video/Data Convergence

Information Assurance Architecture

Current

- Firewalls (Boundary one)
- MIDAS
  - Network IDS
  - Host IDS
  - Virus
  - Cyber Response
  - Red Team (VAP)
- DSID
- MARFOR-CND

Future

- VPN (COI, Boundary 2/3)
- PKI (Boundary 4)
- Application IATO

Crunchy on the outside…
Soft on the inside

Information Architecture

Current

- Global Email Directory
- MCEN Wide NT Standards
- DMS
- Application Dev./Sus.
- Mainframe Issues (HOD, Legacy Apps, Printers)

Future

- Windows 2000
- Collaborative Planning
- Knowledge Mgmt
- Active Directory
- DMS-COC
- Application LCM (Bandwidth, Security, Standards)

MCEN FUTURE ARCHITECTURE

“The man that rests on his laurels, soon finds himself resting six feet under”

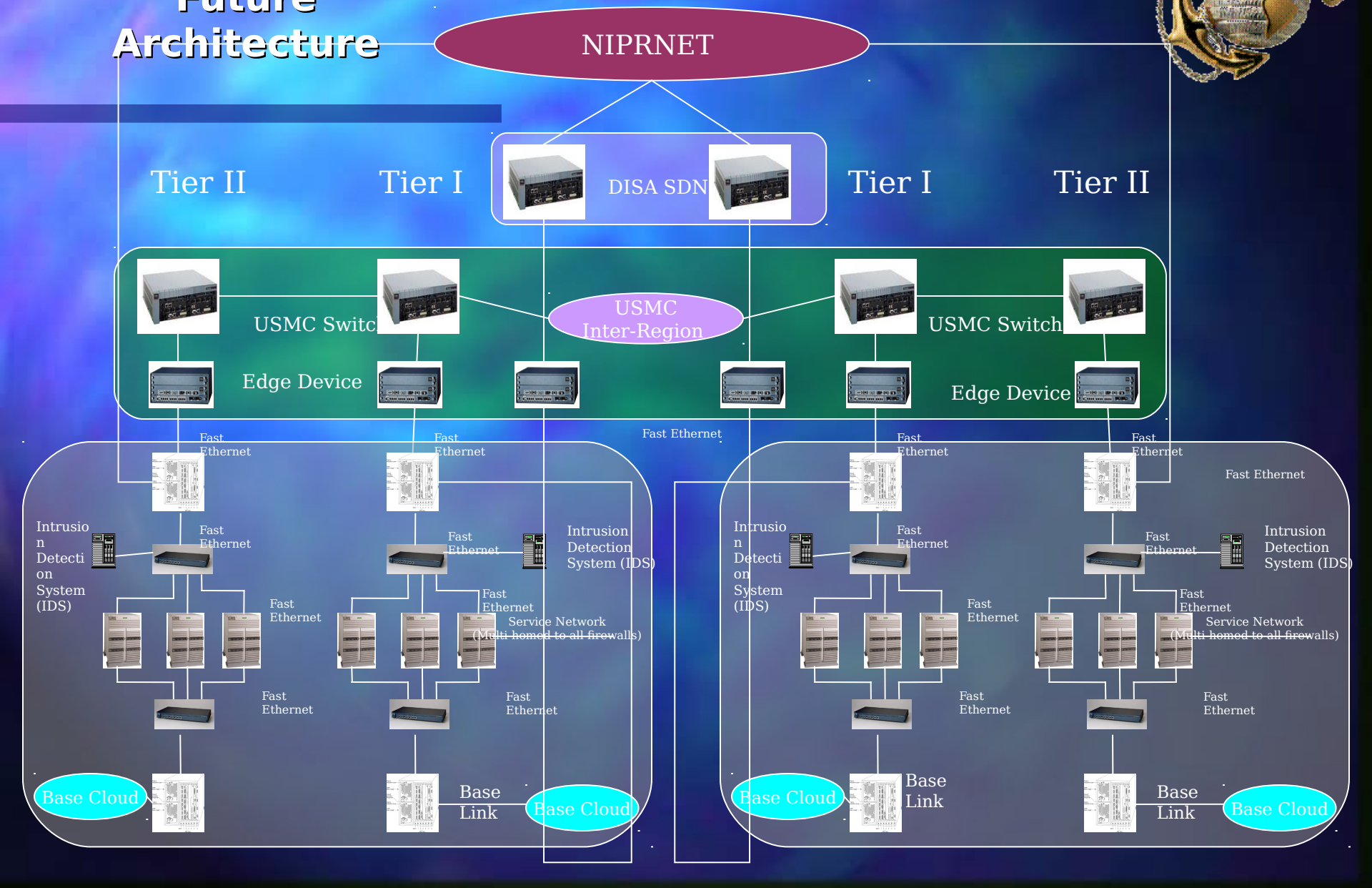
Col. Mike Cooper (USMC, Ret)
Former USMC Deputy CIO

Bandwidth Enhancement Initiative

Oct 98’

- Provide data flow management capabilities to the USMC NOC to be able to conduct traffic shaping.
- Provide the ability to distinguish between USMC traffic and “other” traffic to ensure that the official Marine Corps traffic will not have to compete when traversing the USMC Intranet.
- Provide enough bandwidth to successfully implement high throughput applications, such as distance learning.
- Ensure compatibility with each base ADN, the Navy’s N/MCI initiative and DISN.

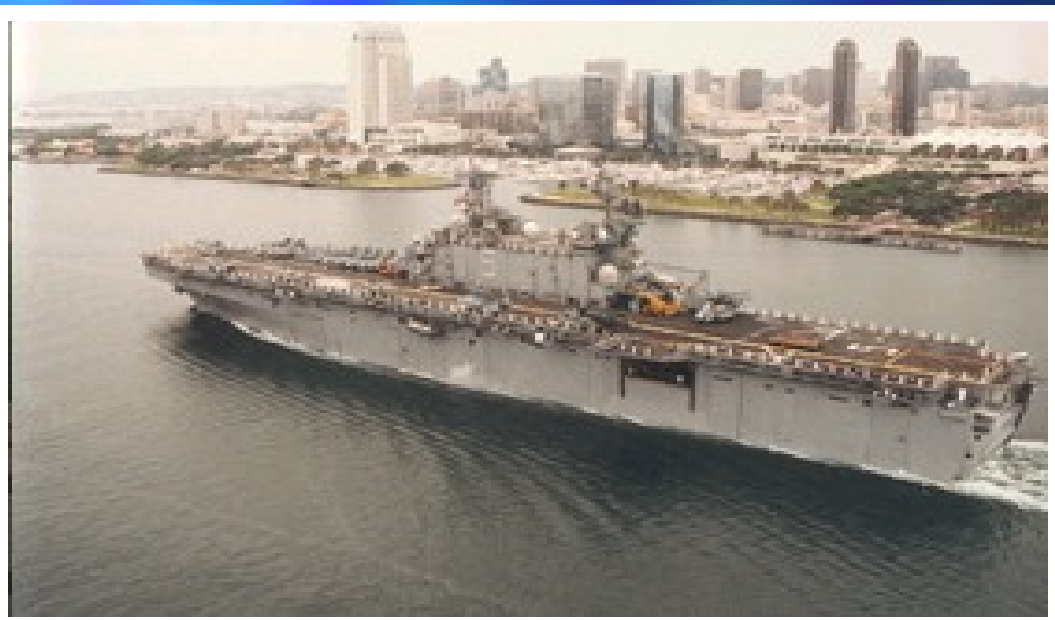
MCEN
Future Architecture



DEPLOYED SUPPORT

“The operating forces are our focus of effort”

ALMAR 023/99 32nd Commandant’s Planning Guidance



Deployed Support

- Leverages off the expertise and resources within the MITNOC to support Marines around the Globe
- Acts as Operational Force liaison with Joint committees, helping to enforce standards
- Deployed Security Interdiction Device (DSID) gives the Marine Deployed Forces the same look and feel as the Garrison units.

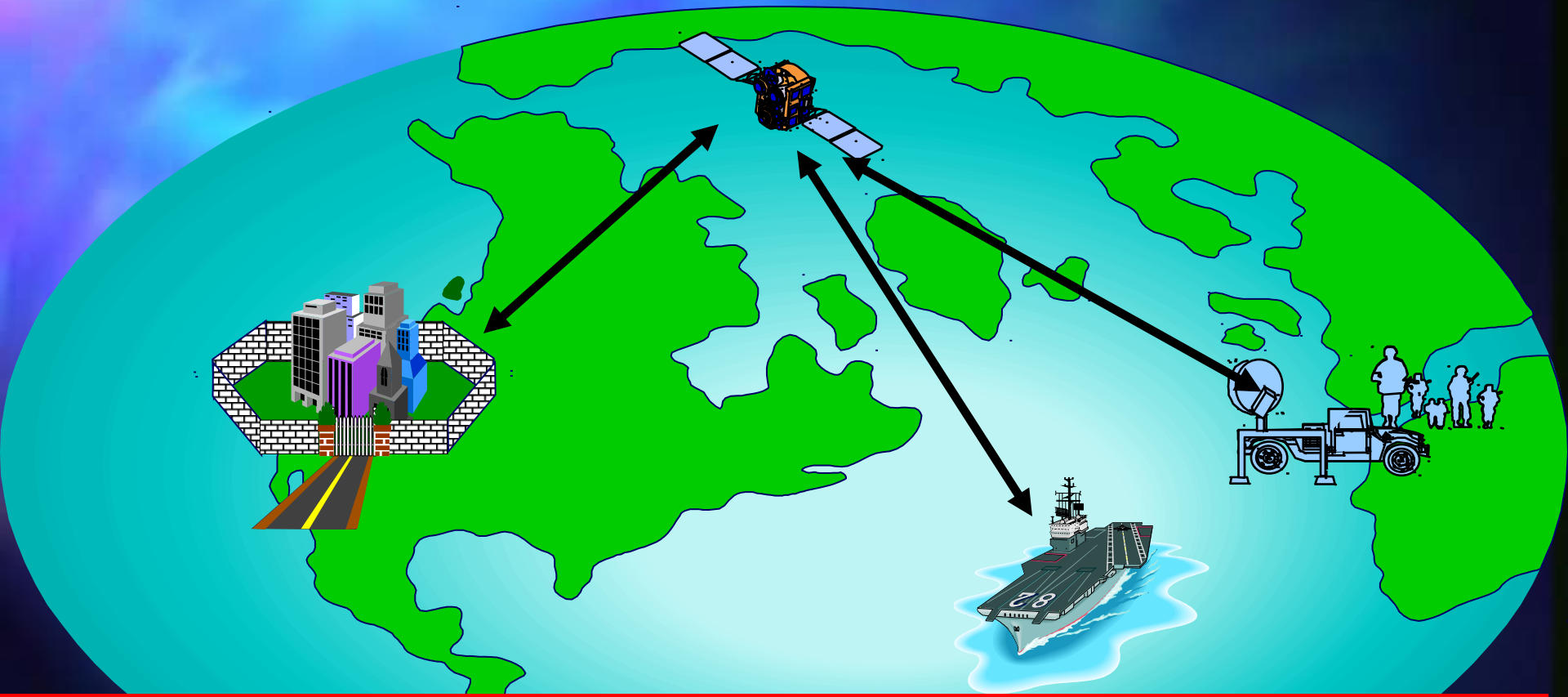
Deployed Support Recent Victories

- East Timor
- TransLANT support with MEU
- Ulchi Focus Lens (UFL) support
- MITNOC touch Labor deploy with IIIMEF in support of Cobra Gold 2000.
- DSID Tactical training conducted to Fleet units by MITNOC Mobile Training Team

Future Deployed Support

- Joint Vision 2010
  - “Whitehouse to Foxhole”
- Operational Maneuver From the Sea (OMFTS)
  - Extension from ship to shore
- MITNOC currently setting the stage for an easy transition by standardizing the tactical as our Garrison, and following the “Train as you fight” mentality.

Projecting Virtual Staffs
JV2010/OMFTS



Security Centric Solutions

MCEN
DEFENSE-IN-DEPTH STRATEGY

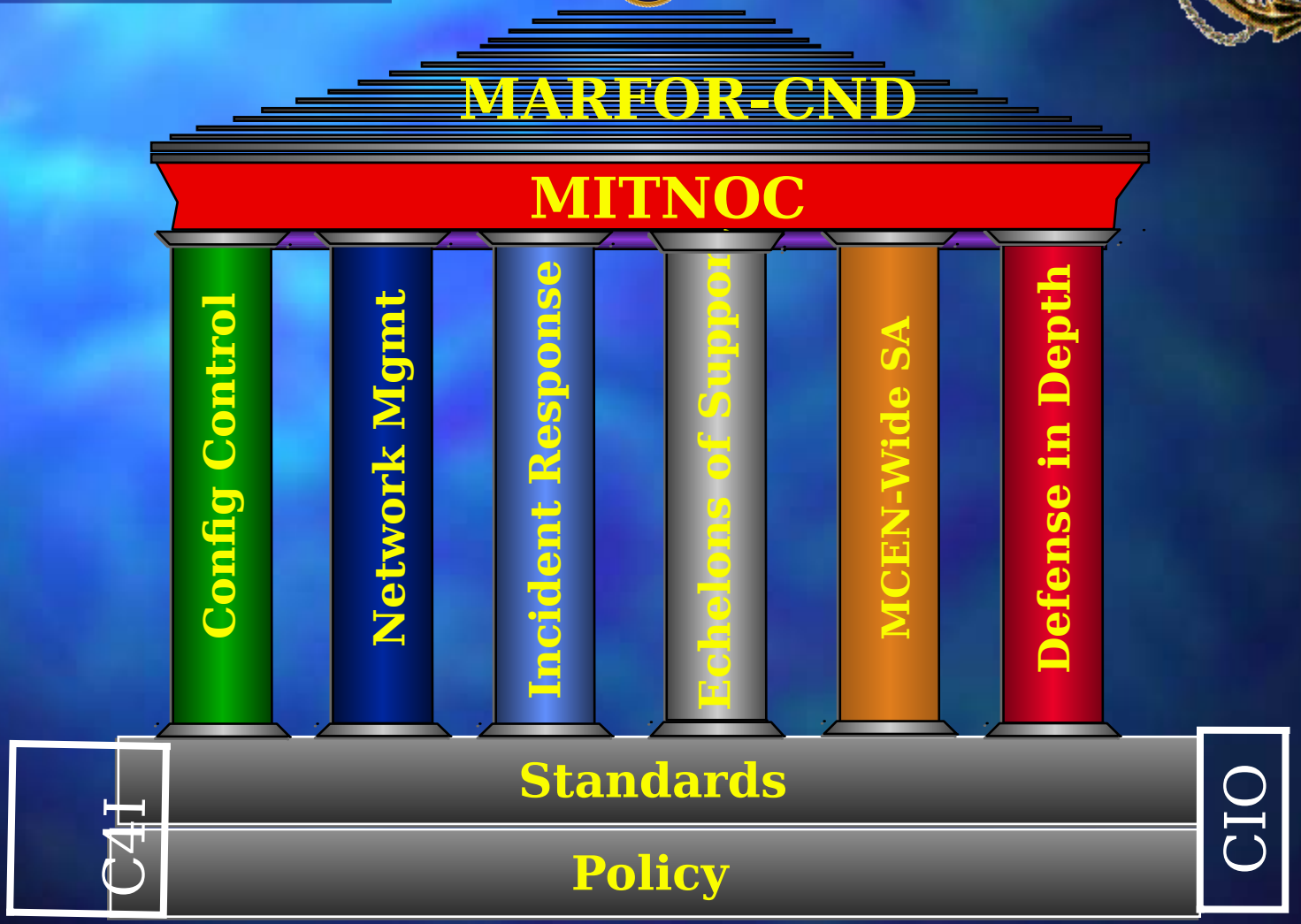
“In God We Trust, all others we monitor”
MITNOC Security Section

How do you successfully manage and secure an enterprise network?

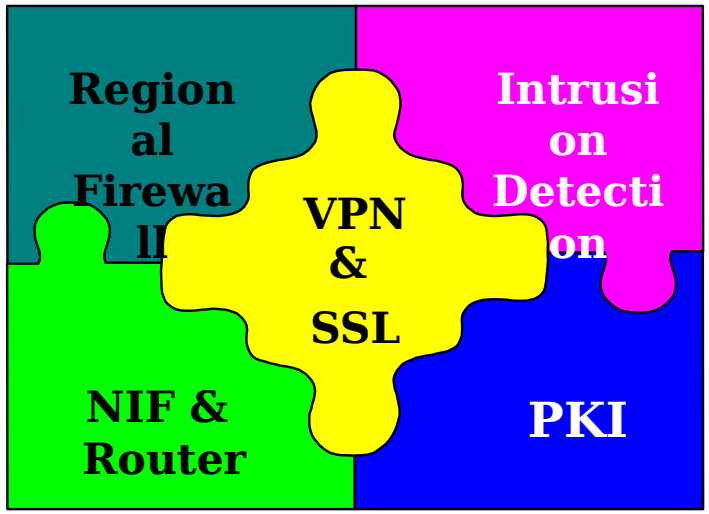
- Senior Leadership Involvement
  - Policy
  - Funding
  - Who's in charge (Bring discipline to the process)
- Centralized Configuration Control and Management
  - Provides for acquisition economies of scale & represents significantly diminished lifecycle management costs
- Centralized Execution
  - Destroy "rice bowl" mentality where possible
- Commitment to Appropriate Staffing

Defending the Network

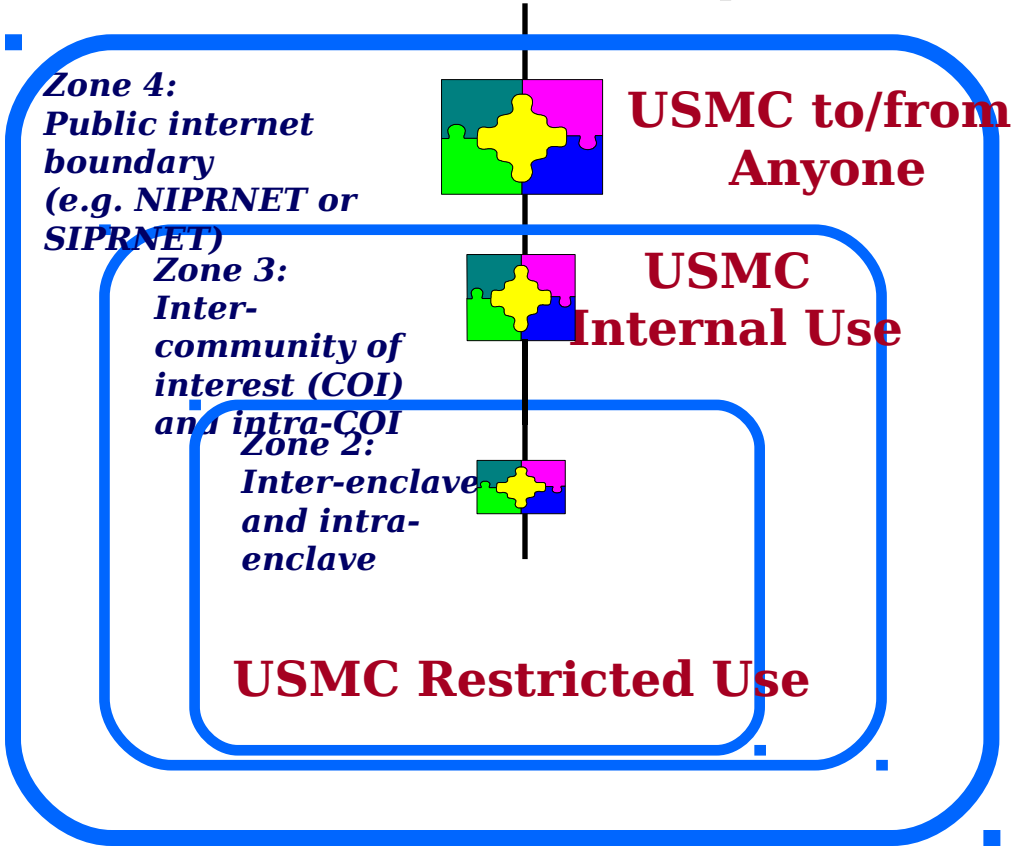
Our Integrated Activities



Objective: Enhanced Boundary Protection, Community of Interest Separation, & Zone Based Protocol Use



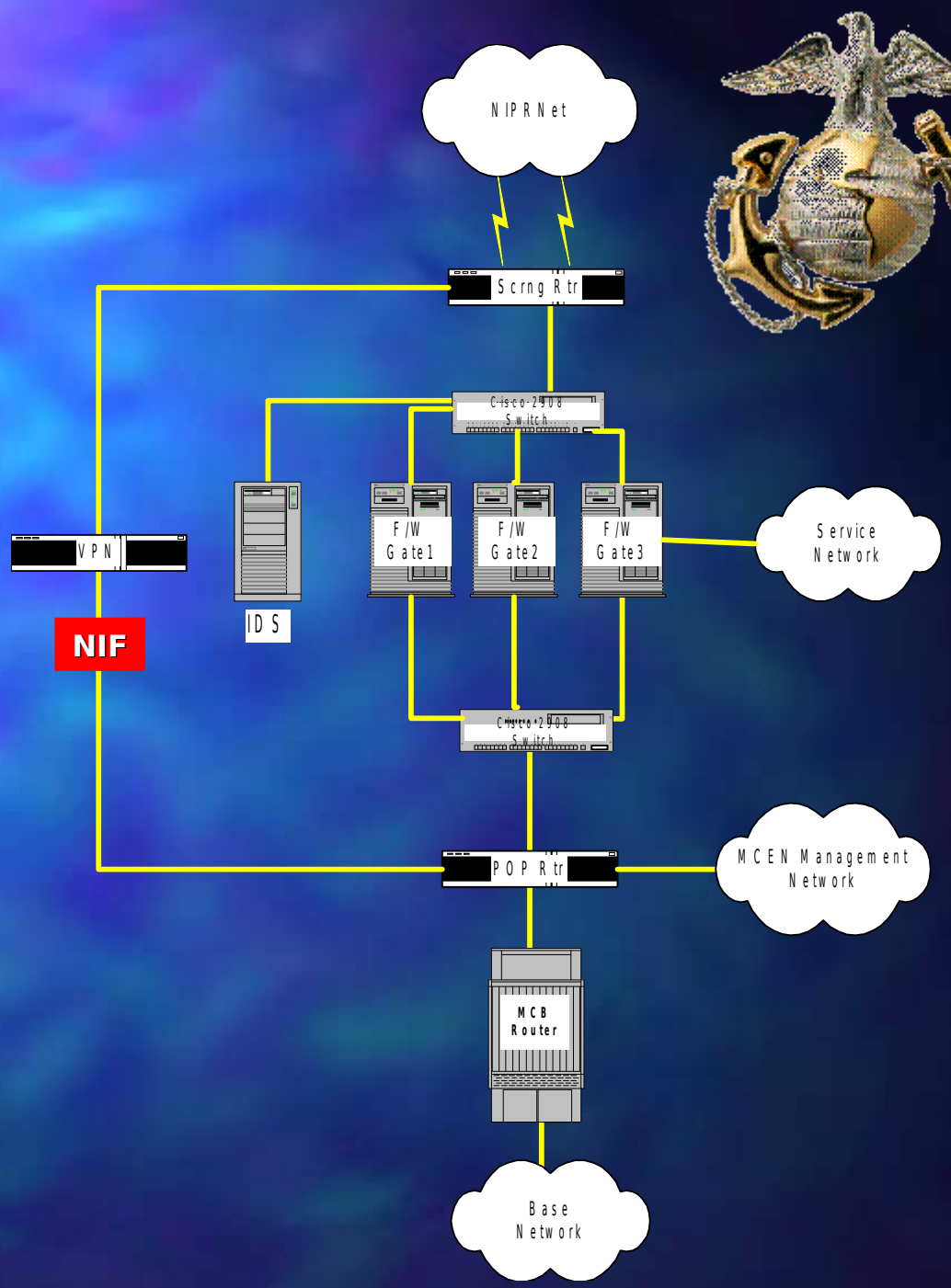
Defense-in-Depth



A USMC Standard Integrated Security System

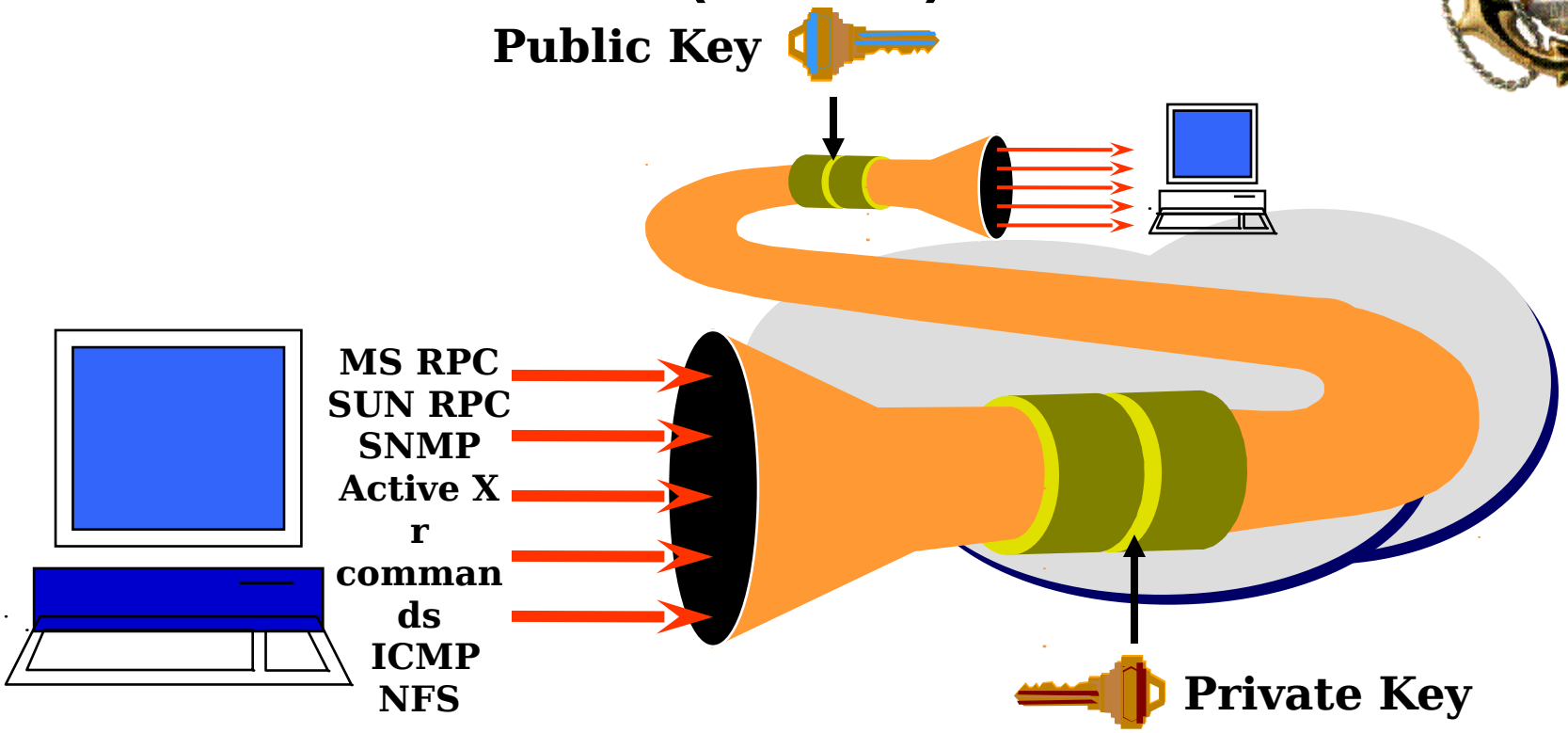
MCEN Firewall Architecture

- Defense-in-Depth Strategy
- That which is not strictly permitted is denied
- IDS Technology
- VPN Technology




eployed Security Interdiction Device
Security at the Network Boundary
MITNOC
Providing Expeditious Support to the Fleet Mari

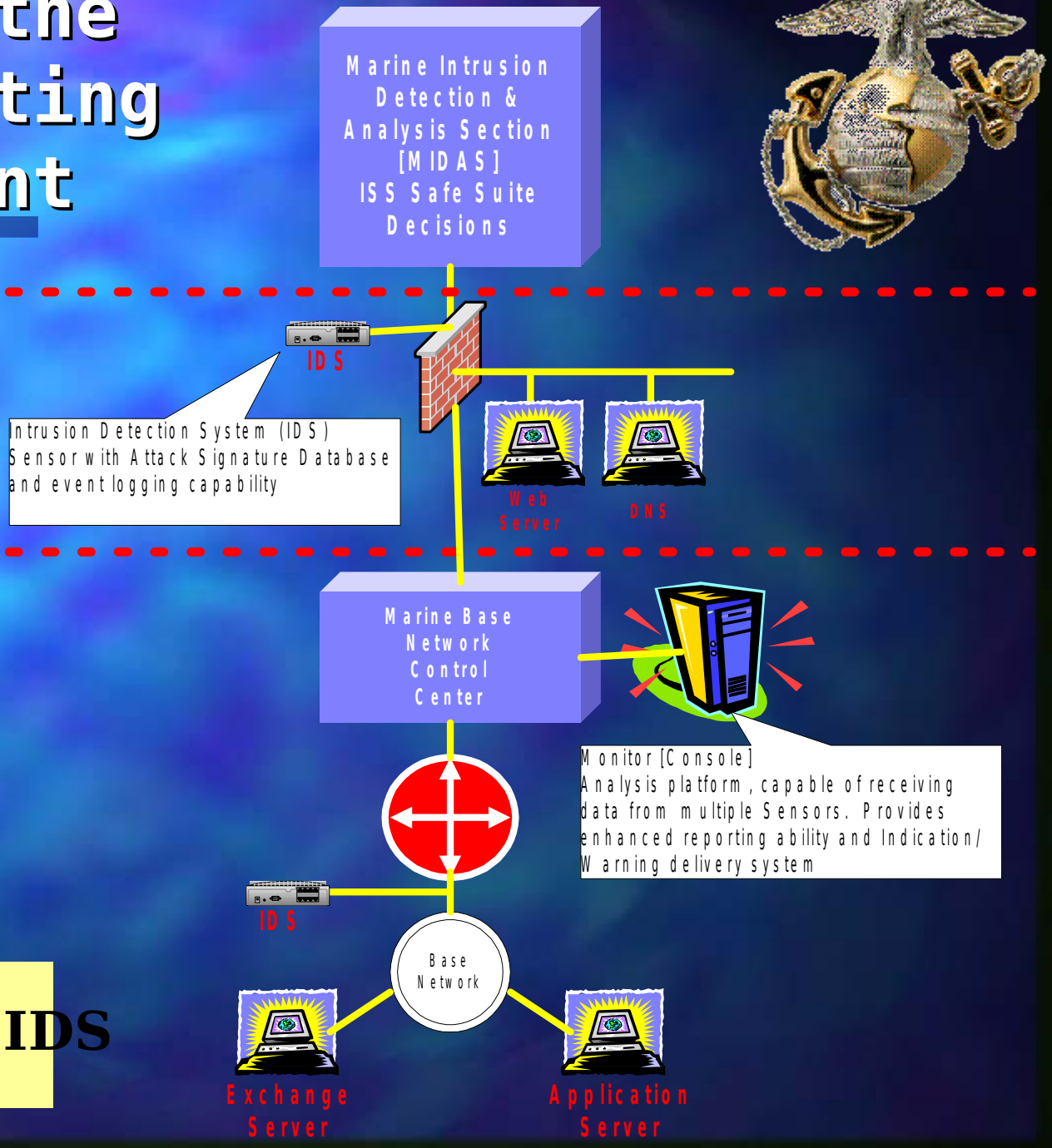
USMC Virtual Private Network (VPN)



- IP Packet Level Encryption Devices (IPSec) or Layer 2 Tunneling
- Confidentiality & Integrity of Data in Transit
- PKI Based Mutual Authentication
- Containment Field for Dangerous Protocols

Defending the Local Computing Environment

- Base Network Infrastructure Protection Suite [BNIPS]
  - Strategic BAN IDS
  - Host IDS [on all servers]
  - Vulnerability



Assessment

Host Level IDS

MITNOC/MARFOR-CND Synergy

- Truly global connectivity, intrusion detection, protection, and defense across the MCEN.
- No physical or organizational separation between CND, network security and daily network management sections.
- Authority to direct action and enforce policy in defense of the MCEN.
- Centralized 24x7 visibility of MCEN day-to-day and defense operations.
- Several shared (dual-hat) positions between the MITNOC and MARFOR staffs (G3/G6, OPSO).
- Built-in surge capability for crisis action periods.

Case Study One:

Human Factor Vulnerability

Disinformation Attack

- Unidentified man purchases 400K of stock in pharmaceutical company for $8.40 per share
- Subject leverages IIS exploit vulnerability on company website, inserting press release announcing that they company was to be purchased by large rival pharmaceutical company
- Stock increases to $57.00 per share within 4 hours of market opening
- Subject walks away with 3 million

Case Study Two:
Cyber Extortion

- Leading E-Commerce company generates average 100K profit per hour per day
- Hacker Group going by CyberPunks out of Pakistan perform highly effective DoS attack for 2 hours on e-commerce site
- E-Commerce company is contacted and told that the DoS attack will stop for 60K. The company is also told that they will not be approached for another 12 months
- Company Pays, Does NOT inform FBI
- CyberPunks later contact company offering security services on prevention of DoS

Case Study Three:
Cyber Espionage

- Company A is leading E-Commerce B2B provider in competitive large market segment
- Company A strategic offering is competitive on-line catalog with 900,000 products
- Company B exploits web vulnerability and resets backend catalog prices to a discount of 60%
- Company A loses 600K
- Company B is in non-extradition country

Case Study Four:
Information Warfare Scenario

- New USMC logistical system replaces legacy MIMMS/SASSY – application provides significantly improved functionality to users. System is considered mission critical and unclassified.
- Application uses Telnet and FTP for primary management & transmission protocols. FTP/Telnet are known high risk protocols.
- During Kosovo operation, pro-Serbian hackers access logistic system via anonymous Telnet session. Through poor system security they are able to download the /pwd file which was subsequently broken using LOPHT crack.
- Much later, Supply officer discovers that vast amounts of information have been down loaded and replaced. Forensic investigation determines that the system has also been loaded with sniffer software and multiple Trojan horses including the new ZOMBIE DoS exploit.
- Recovery time is approximately 1600 hours as a complete revalidation of mainframe data is required. Cost to government is estimated at 600K.

USMC Network Security

“The beach is secured, we’re moving inland”